WHAT IS CLAIMED IS:

1. A method for encoding and authenticating a streamed transmission of an electronic file, the method including:

generating a progression of check values, each check value in the progression being derived from at least one other check value in the progression and from a hash of a portion of the electronic file;

encrypting a root check value in the progression of check values;

transmitting the electronic file and the progression of check values to a user's system via a data stream; and

receiving and authenticating the data stream, including:

receiving the root check value;

decrypting the root check value; and

using the decrypted root check value and one or more received check values in the progression of check values to authenticate portions of the data stream, whereby portions of the data stream are authenticated before the entire electronic file and the entire progression of check values are received by the user's system.

2. A method as in claim 1, in which each check value in the progression of check values comprises a hash of (i) at least one other check value in the progression, and (ii) a hash of a portion of the electronic file.

3. A method for encoding and authenticating a data block in a fault-tolerant fashion, the method including:

(1) encoding the data block, the encoding including:

LAW OFFICES
FINNEGAN, HENDERSON, FARABOW, GARRETT, & DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

(a) hashing a first portion of the data block to obtain a first hash value;

(b) hashing a combination of the first hash value and a first verification value to obtain a second verification value, wherein the first verification value is derived, at least in part, from a hashed portion of the data block and a third verification value;

(c) encrypting the second verification value;

(2) transmitting an encoded data stream to a receiver, wherein the encoded data stream includes the encrypted second verification value, the first hash value, the first portion of the data block, and the first verification value; and

(3) receiving the encoded data stream and verifying its integrity, including:

(a) receiving the encrypted second verification value;

(b) decrypting the encrypted second verification value;

(c) receiving the first hash value, a first portion of the encoded data stream, and the first verification value;

(d) hashing the first portion of the encoded data stream to obtain a first re-computed hash;

(e) comparing the first re-computed hash with the first hash value, and, if the first re-computed hash is not equal to the first hash value, hashing a combination of the first hash value and the first verification value to obtain a first calculated hash value; and

(f) comparing the second verification value with the first calculated hash value, and, if the second verification value is equal to the

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

first calculated hash value, releasing the first portion of the encoded data stream for use.

4. A method for encoding and authenticating a data block, the method including:

(1) generating a chain of data verification values, including:

(a) hashing a first sub-block of the data block to obtain a first hash value;

(b) hashing a combination of the first hash value and a first verification value to obtain a second verification value;

(c) hashing a second sub-block of the data block to obtain a second hash value;

(d) hashing a combination of the second hash value and a third verification value to obtain a fourth verification value, wherein the third verification value is derived, at least in part, from the second verification value;

(e) generating a digital signature by signing the fourth verification value using a first cryptographic key;

(2) transmitting an encoded data stream to a receiver, the encoded data stream including the digital signature, the second sub-block, the third verification value, the second verification value, the first sub-block, and the first verification value; and

(3) receiving and verifying the integrity of the encoded data stream, including:

(a) receiving the digital signature;

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

(b) using a second cryptographic key to unsign the digital signature to obtain the fourth verification value;

(c) receiving a first portion of the encoded data stream and the third verification value;

(d) hashing the first portion of the encoded data stream to obtain a first received hash value;

(e) hashing a combination of the first received hash value and the third verification value to obtain a first calculated hash;

(f) comparing the fourth verification value with the first calculated hash;

(g) releasing the first portion of the encoded data stream for use if the fourth verification value is equal to the first calculated hash;

(h) receiving the second verification value;

(i) verifying that the second verification value is securely derived from the third verification value;

(j) receiving a second portion of the encoded data stream and the first verification value;

(k) hashing the second portion of the encoded data stream to obtain a second received hash value;

(l) hashing a combination of the second received hash value and the first verification value to obtain a second calculated hash;

(m) comparing the second verification value with the second calculated hash; and

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

(n) releasing the second portion of the encoded data stream for use if the second verification value is equal to the second calculated hash.

5. A method as in claim 4, in which receiving and verifying the integrity of the encoded data stream further includes:

(3)(o) preventing further processing of the encoded data stream if the second verification value is not equal to the second calculated hash.

6. A method as in claim 4, in which the combination of the first hash value and the first verification value comprises a concatenation of the first hash value and the first verification value.

7. A method as in claim 4, in which:

the digital signature, the second sub-block, and the third verification value are transmitted consecutively in the encoded data stream; and

the second verification value, the first sub-block, and the first verification value are transmitted consecutively in the encoded data stream.

8. A method as in claim 4, in which the first cryptographic key is identical to the second cryptographic key.

9. A method as in claim 4, in which the first cryptographic key comprises a sender's private key, and in which the second cryptographic key comprises the sender's public key.

10. A method as in claim 4, in which the first verification value comprises a predefined data pattern.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

11. A method as in claim 4, in which the encoded data stream further includes the second hash value, and in which receiving and verifying the integrity of the encoded data stream further includes:

(3)(c)(1) receiving the second hash value;

(d)(1) replacing the first received hash value with the second hash value if the first received hash value is not equal to the second hash value.

12. A method as in claim 4, in which the encoded data stream further includes the second hash value, and in which receiving and verifying the integrity of the encoded data stream further includes:

(3)(c)(1) receiving the second hash value;

(g)(1) if the fourth verification value is not equal to the first calculated hash, generating a first recovered hash value by hashing a combination of the second hash value and the third verification value;

(g)(2) comparing the fourth verification value with the first recovered hash value;

(g)(3) releasing the first portion of the encoded data stream for use if the fourth verification value is equal to the first recovered hash value.

13. A method as in claim 12, in which receiving and verifying the integrity of the encoded data stream further includes:

(g)(4) preventing further processing of the encoded data stream if the fourth verification value is not equal to the first recovered hash value.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

14. A method for encoding a block of content in a manner designed to facilitate authentication, the method including:

(a) hashing a first portion of the block of content to obtain a first hash value;

(b) hashing a combination of the first hash value and a first data verification value to obtain a second verification value;

(c) hashing a second portion of the block of content to obtain a second hash value;

(d) hashing a combination of the second hash value and a third verification value to obtain a fourth verification value, wherein the third verification value is derived, at least in part, from the second verification value;

(e) generating a digital signature by signing the fourth verification value using a cryptographic key; and

(f) sending the digital signature, the second portion of the block of content, the third verification value, the second verification value, the first portion of the block of content, and the first verification value to a computer readable storage device.

15. A method as in claim 14, in which the first verification value is derived, at least in part, from a third portion of the block of content.

16. A method for encoding and transmitting a digital file in a manner designed to facilitate authentication of a streamed transmission of the file, the method including:

generating a progression of check values, each check value in the progression being derived from at least one other check value in the progression and from a transformed portion of the file; and

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

transmitting the digital file and the progression of check values to a user's system, whereby the user's system is able to receive portions of the file and to use one or more received check values to authenticate said portions of the file before the entire file is received.

17. A method as in claim 16, further including:

encrypting a final check value in the progression of check values;

wherein the step of generating an encoded file includes inserting the final check value into the file in proximity to the beginning of the file.

18. A method as in claim 16, in which the transformed portion of the file comprises a hashed portion of the file.

19. A method as in claim 18, in which generating the encoded file further includes:

inserting a plurality of hash values into the file, each hash value comprising a hash of a portion of the file, and each hash value being inserted in proximity to the portion of the file to which it corresponds.

20. A method for encoding a block of content in a manner designed to facilitate authentication, the method including:

(a) performing a first operation on a first portion of the block of content to obtain a first transformed value;

(b) performing a second operation on a first input and the first transformed value to obtain a first check value;

(c) performing the first operation on a second portion of the block of content to obtain a second transformed value; and

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

(d) performing the second operation on a second input and the second transformed value to obtain a second check value, wherein the second input is derived, at least in part, from the first check value;

(e) generating a digital signature by signing the second check value using a cryptographic key; and

(f) sending the digital signature, the second portion of the block of content, the second input, the first check value, the first portion of the block of content, and the first input to a computer readable storage device.

21. A method as in claim 20, in which the computer readable storage device is one of: CD-ROM, DVD, MINIDISC, floppy disk, magnetic tape, flash memory, ROM, RAM, system memory, hard drive, optical storage, and a data signal embodied in a carrier wave.

22. A method as in claim 20, in which the first operation comprises a one-way hashing function.

23. A method as in claim 20, in which the first operation is selected from a group consisting of: the SHA-1 hashing function; the MD4 hashing function; the MD5 hashing function; the RIPE-MD hashing function; and a message authentication code function.

24. A method as in claim 22, in which the second operation comprises concatenating two values and hashing the result.

25. A method as in claim 20, in which the first input comprises a predefined data pattern.

26. A method as in claim 20, in which the first input is derived, at least in part, from a third portion of the block of content.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

27. A method as in claim 20, in which the content includes audio, video, textual, or multimedia data.

28. A computer program product for encoding a data block in a manner designed to facilitate authentication of a streamed transmission of the data block, the computer program product including:

(a) computer code for generating a progression of data check values, wherein each data check value is derived, at least in part, from (i) at least one other data check value in the progression, and (ii) a hash of a portion of the data block;

(b) computer code for encoding the data block by inserting each data check value into the data block in proximity to a portion of the data block to which the data check value corresponds;

(c) computer code for sending a streamed transmission of the encoded data block to a user's system, whereby the user's system is able to receive and authenticate portions of the streamed transmission before all of the data block is received; and

(d) a computer readable medium for storing the computer codes.

29. A computer program product as in claim 28, further including:

(a)(1) computer code for digitally signing at least a root data check value in the progression of data check values.

30. A computer program product as in claim 28, in which the computer readable medium is one of: CD-ROM, DVD, MINIDISC, floppy disk, magnetic tape, flash memory, ROM, RAM, system memory, hard drive, optical storage, and a data signal embodied in a carrier wave.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

31. A method for verifying the integrity of data contained in a data stream, the method including:

(a) receiving an encrypted first check value, the encrypted first check value being derived, at least in part, from a second check value, a third check value, a fourth check value, and the data;

(b) decrypting the encrypted first check value;

(c) receiving a first block of data and the second check value;

(d) obtaining a first calculated check value by performing a predefined operation on a combination of (i) a value derived from the first block of data, and (ii) the second check value;

(e) comparing the first check value with the first calculated check value;

(f) allowing at least one use of the first block of data if the first check value is equal to the first calculated check value;

(g) receiving the third check value, a second block of data, and the fourth check value;

(h) obtaining a second calculated check value by performing the predefined operation on a combination of (i) a value derived from the second block of data, and (ii) the fourth check value;

(i) comparing the third check value with the second calculated check value; and

(l) allowing at least one use of the second block of data if the third check value is equal to the second calculated check value.

32. A method as in claim 31, in which the at least one use of the first block of data includes one of: sending the first block of data to a speaker system; displaying the

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

first block of data on a viewing device; printing the first block of data; and storing the first block of data on a computer readable medium.

33. A method as in claim 31, in which the predefined operation comprises a hashing operation.

34. A method as in claim 33, in which the combination of (i) the value derived from the first block of data and, (ii) the second check value comprises a concatenation of the second check value with a hash of the first block of data.

35. A method as in claim 31, in which the second check value is derived, at least in part, from the third check value, and in which the third check value is derived, at least in part, from the fourth check value.

36. A computer program product for verifying the integrity of a block of data, the computer program product including:

computer code for receiving a first portion of the block of data, and for receiving first and second check values in a chain of check values, wherein each check value in the chain is derived from a corresponding transformed portion of the block of data and from at least one other check value in the chain;

computer code for verifying the integrity of the first portion of the block of data and the second check value using, at least in part, the first check value;

computer code for allowing at least one use of the first portion of the block of data if the integrity of said first portion is successfully verified; and

a computer readable medium for storing the computer codes.

37. A computer program product as in claim 36, in which the first check value is digitally signed, and in which the computer code for verifying the integrity of the first portion of the block of data and the second check value includes computer code for unsigning the first check value.

LAW OFFICES
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

38. A computer program product as in claim 36, in which each transformed portion of the block of data is obtained by hashing said portion of the block of data.

39. A computer program product as in claim 36, further including:

computer code for receiving a first transformed value corresponding to the first portion of the block of data; and

computer code for using the first transformed value and the first check value to verify the integrity of the second check value.

40. A computer program product as in claim 39, further including:

computer code for allowing at least one use of the first portion of the block of data if verification of the integrity of less than a predefined number of portions of the block of data has failed.

41. A computer program product as in claim 39, in which the first transformed value comprises a hash of the first portion of the block of data.

42. A computer program product as in claim 36, in which the at least one use of the first portion of the block of data is selected from a group consisting of: sending the first portion of the block of data to a speaker system; displaying the first portion of the block of data on a viewing device; printing the first portion of the block of data; and storing the first portion of the block of data on a computer readable medium.

43. A system for performing fault-tolerant authentication of a stream of data, the system including:

(a) a receiver for receiving sub-blocks of the stream of data, error-check values corresponding to the sub-blocks, and verification values in a chain of verification values associated with the stream of data, wherein each verification value in the chain is derived, at least in part, from (i) a sub-

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

block of the stream of data, and (ii) at least one other verification value in the chain;

(b) error-detection logic operable to use a received error-check value to detect errors in a corresponding sub-block of the stream of data;

(c) error-handling logic operable to record the detection of errors by the error-detection logic, and to block the receipt of additional sub-blocks if a predefined error condition is satisfied; and

(d) authentication logic operable to use a first received verification value to verify the integrity of a second received verification value and one of (i) a received sub-block of the data stream, and (ii) a received error-check value.

44. A system as in claim 43, in which the predefined error condition is the detection of more than a predefined number of errors by the error-detection logic.

45. A system as in claim 43, in which the predefined error condition is the detection of a predefined pattern of errors by the error-detection logic.

46. A system as in claim 43, in which at least a portion of the receiver, error-detection logic, error-handling logic, or authentication logic comprise computer code stored on a computer readable medium.

47. A system as in claim 43, in which the error-detection logic includes:

hashing logic for computing a hash of a sub-block of the stream of data;

comparison logic for comparing the hash of the sub-block with a received error-check value.

48. A method for authenticating data, the method including:

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

(a) receiving a first sub-block of the data, a first error-check value, a first check value, and a second check value, wherein the first check value and the second check value form part of a progression of check values associated with the data, each check value in the progression being derived, at least in part, from (i) a sub-block of the data, and (ii) at least one other check value in the progression;

(b) using the first error-check value to detect a corruption of the integrity of the first sub-block;

(c) recording the detection of the corruption; and

(d) using the first check value and the first error-check value to verify the integrity of the second check value.

49. A method as in claim 48, further including:

(e) receiving a second sub-block of the data;

(f) using the second check value to verify the integrity of the second sub-block.

50. A method as in claim 48, wherein each check value in the progression is derived, at least in part, from a transformed sub-block of the data.

51. A method as in claim 48, in which the first error-check value comprises a hash of the first sub-block of the data.

52. A method for encoding a block of data in a manner designed to facilitate fault-tolerant authentication, the method including:

generating a progression of check values, each check value in the progression being derived from a portion of the block of data and from at least one other check value in the progression;

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

generating an encoded block of data, including:

inserting each check value of the progression into the block of data, each check value being inserted in proximity to a portion of the block of data to which it corresponds; and

inserting error-check values into the block of data, each error-check value being inserted in proximity to a portion of the block of data to which it corresponds, and each error-check value being operable to facilitate authentication of a portion of the block of data and of a check value in the progression of check values;

transmitting the encoded block of data to a user's system, whereby the user's system is able to receive and authenticate portions of the encoded block of data before the entire encoded block of data is received.

53. A method as in claim 52, in which each error-check value comprises a hash of the portion of the block of data to which it corresponds.

54. A method as in claim 53, in which each check value in the progression comprises the hash of a combination of at least (i) a hash of the portion of the block of data to which it corresponds, and (ii) another check value in the progression.

55. A method for securely accessing a data block, the method including:

selecting a portion of the data block;

loading a root verification value and one or more stored check values in a hierarchy of check values into a memory unit, wherein the hierarchy of check values is derived, at least in part, from an uncorrupted version of the data block;

verifying the integrity of the one or more stored check values using, at least in part, the root verification value;

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

generating a calculated check value by performing a transformation on a first sub-block of the data block, the first sub-block including at least part of the selected portion of the data block;

comparing the calculated check value with a first verified stored check value; and

releasing at least part of the selected portion of the data block for use if the calculated check value equals the first verified stored check value.

56. A method as in claim 55, in which the memory unit comprises a stack.

57. A method as in claim 55, in which the root verification value is obtained by decrypting a digital signature associated with the data block.

58. A method as in claim 55, in which the root verification value is derived, at least in part, from the check values in the hierarchy of check values.

59. A method as in claim 55, in which the memory unit is tamper-resistant.

60. A method as in claim 55, in which the hierarchy of check values comprises a tree data structure.

61. A method as in claim 60, in which the tree data structure is symmetric.

62. A method as in claim 61, in which the tree data structure has a branching factor of four.

63. A method as in claim 55, further including:

inhibiting at least one use of the selected portion of the data block if the calculated check value is not equal to the first verified stored check value.

64. A method as in claim 55, in which verifying the integrity of the one or more stored check values includes:

LAW OFFICES
FINNEGAN, HENDERSON, FARABOW, GARRETT, & DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

using the root verification value to verify the integrity of a second stored check value in the hierarchy of check values; and

using the second stored check value to verify the integrity of a first stored check value.

65. A method as in claim 1, in which using the second stored check value to verify the integrity of the first stored check value includes:

comparing the second stored check value with a calculated group check value, wherein the calculated group check value is obtained by combining the first stored check value with at least one other check value at the same level in the hierarchy of check values as the first stored check value.

66. A method as in claim 55, in which the first verified stored check value comprises a first hash value, and in which the calculated check value comprises a second hash value obtained by hashing the first sub-block.

67. A method as in claim 55, whereby a user can select a first portion of the data block, and whereby the selected portion of the data block can be authenticated using the root verification value without authenticating the entire data block.

68. A method as in claim 67, whereby the user can select a second portion of the data block, and whereby the second portion of the data block can be authenticated using the root verification value without re-authenticating the first portion of the data block.

69. A system for providing secure access to a data file, the system including:

a memory unit for storing a digital signature and a plurality of hash values related to the data file, wherein the digital signature and the plurality of hash values form a hierarchy;

a processing unit;

LAW OFFICES
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

decryption logic for decrypting the digital signature to obtain a root verification value;

hash verification logic for using the root verification value to verify the integrity of at least a first stored hash value in the hierarchy;

selection logic for selecting a portion of the data file;

a hashing engine for calculating a hash of a data sub-block, the data sub-block including at least part of the selected portion of the data file;

a first comparator for comparing the calculated hash with the first stored hash value; and

control logic for releasing the data sub-block for use if the calculated hash equals the first stored hash value.

70. A system as in claim 69, in which at least one of the decryption logic, the hash verification logic, the selection logic, the hashing engine, the first comparator, and the control logic are implemented in software executed by the processing unit.

71. A method for encoding a digital file in a manner designed to facilitate secure, quasi-random access to said digital file, the method including:

generating a multi-level hierarchy of hash values from the digital file, wherein one or more hash values on a first level of the hierarchy are derived, at least in part, from a plurality of hash values on a second level of the hierarchy;

digitally signing a root hash value, the root hash value being derived, at least in part, from each of the hash values in the hierarchy; and

storing the signed root hash value and a predefined number of levels of the multi-level hierarchy of hash values on a computer readable medium.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

72. A method as in claim 71, in which generating the multi-level hierarchy of hash values includes:

hashing a first portion of the digital file to obtain a first hash value;

hashing a second portion of the digital file to obtain a second hash value;

combining at least the first and second hash values to yield a third hash value;

wherein the first and second hash values comprise at least part of said second level of the multi-level hierarchy of hash values, and wherein the third hash value comprises at least part of said first level of the hierarchy of hash values.

73. A method as in claim 72, in which combining at least the first and second hash values includes concatenating at least the first and second hash values and hashing the result.

74. A method as in claim 71, whereby at least a portion of the hierarchy of hash values can be retrieved and used to authenticate an arbitrarily-selected portion of the digital file.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000